Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

20. (Currently Amended) A method for protecting the processing of sensitive information in a security module having a monolithic structure comprising at least an information processing device, a storage device for storing information capable of being processed by said processing device and at least a data bus, the security module further comprising means for checking the integrity of information, said means for checking the integrity being either a table contained in the processing device or a plurality of software program instructions of the storage device or a specific hardware circuit, wherein the transmitting of information through said data bus is secured by the method comprising at least the following steps:

[[-]]selecting a piece of sensitive information stored in the storage device addressed by the processing device;

[[-]]determining, by the means for checking the integrity, a specific condition for establishing the integrity of a datum of said sensitive information to be transmitted on said data bus;

[[-]]transferring reading by the processing device of said a datum of said sensitive information transmitted from the storage device to the processing device, on said data bus;

[[-]]processing said datum and verifying executing a logic verification operation on all bits of said datum which is transmitted transferred on said data bus, by said processing device or by said means for checking the integrity, of information, during the processing for verifying that said specific condition is satisfied; and

[[-]]disabling the processing of said sensitive information by the processing device if the specific condition is not satisfied.

21. (Currently Amended) The method according to claim 20, wherein said ~~information~~ datum of said sensitive information is an operation code datum read in the storage device, ~~all of the types of~~ said operation code datum being recognized ~~contained~~ in said [[a]] table contained in the processing device ~~having a content determined during the manufacture of the security module~~, said specific condition ~~for the integrity of the information~~ being satisfied if said operation code datum is equal to a valid operation code datum of the table and said specific condition is not satisfied at least if one or more bits of the operation code datum ~~data composed by bits~~ are all equal to a same binary value ~~are non-valid operation code data of the table~~.

22. (Cancelled)

23. (Currently Amended) The method according to claim 20, wherein said means for checking the integrity ~~of information~~ comprises a ~~logic comparator and~~ first and a second logic operator disposed in an entry and an output ~~each at different terminations~~ of the data bus, ~~said logic operators~~ respectively, and producing ~~at least respectively~~ a first and a second result, respectively, the means for checking the integrity further comprising a logic comparator for comparing said first and second result, ~~compared together by said logic comparator~~ and for verifying said specific condition for the integrity by checking ~~when there is~~ an equality between said first and second results.

24. (Cancelled)

25. (Cancelled)

26. (Currently Amended) The method according to claim 20, wherein the disabling of the <u>processing of said sensitive information comprises the disabling of the </u>processing device [[is]] performed by executing a microprogrammed instruction.   ·

27. (Previously Presented) The method according to claim 26, wherein said microprogrammed instruction induces the following steps:

　　- writing a piece of disable data into a non volatile location of the storage device; and

　　- disabling the processing device.

28. (Currently Amended) The method according to claim 27<u>, wherein said microprogrammed instruction</u> further ~~comprising~~<u>comprises the </u>reading by the processing device <u>at </u>said non volatile location of the storage device upon power up of said module<u>, </u>before disabling the processing device if a value read at this location does not match.

29. (Currently Amended) A security module comprising an electronic circuit having a monolithic structure and comprising an information processing device, an information storage device communicating with said processing device via a data bus, the processing device selecting <u>sensitive </u>information data extracted from the storage device in order to process them, <u>the security module further comprising </u>means for checking the integrity of information<u> being either a table contained in the processing device or a plurality of software program instructions of the storage device or a specific hardware circuit</u>, wherein <u>said means for checking the integrity verifies </u>a specific condition for integrity <u>by verifying </u>~~concerning ~~a datum <u>of said sensitive information, transferred </u>~~transmitted ~~on the data bus ~~is verified, by said processing~~

~~device or by said means for checking the integrity of information, by executing a~~

~~logic operation on all bits of said datum which is transmitted on said bus and~~ the

security module further comprising means for disabling the processing of said

sensitive information by the processing device when said specific condition for

integrity is not satisfied.

30. (Currently Amended) The security module according to claim 29, wherein the

datum transferred on the data bus is an operation code datum executed by the

processing device ~~execute instruction data corresponding to operation codes~~

corresponding to an instruction extracted from said [[a]] table, ~~defined during the~~

~~building of the module, wherein~~ the table ~~comprises~~ comprising at least a forbidden

instruction, and wherein said specific condition for integrity is not satisfied when said

processing device process_es said [[a]] forbidden instruction.

31. (Currently Amended) The security module according to claim 30, wherein at

least [[an]] instruction_s [[data]] of said table corresponding to said operation code

datum constituted by bits all ~~whose all bits are~~ equal to a same binary value are

forbidden instructions of said table.

32. (Cancelled)

33. (Currently Amended) The security module according to claim 29, wherein said

means for disabling the processing of said sensitive information [[device]] comprise_s

means for irreversibly writing at least one indicator with an initial valid state in a non

reversible modified invalid state, and means for reading said indicator during the next

power-up of the module and disabling the processing device if an invalid state of said

indicator is read.

34. (Currently Amended) The security module according to claim 29, wherein said means for checking the integrity of information comprises at least a first and a second [[two]] parity generator [[each]] respectively disposed in an entry and an output at terminations of the data bus, and at least one a comparator whose inputs are connected to [[an]] outputs of said first and second parity generators[[,]] for verifyingto verify said specific condition for integrity when said first and second parity generators produce identical outputs, and to set by setting an output of said comparator linked to an interrupt input of [[said]] the processing device.

35. (Currently Amended) The security module according to claim 34, wherein said outputs of bothsaid first and second parity generators [[is]]are set opposite according to a function of time.

36. (Currently Amended) The security module according to claim 34, wherein said outputs of bothsaid first and second parity generators [[is]]are set opposite randomly.

37. (Previously Presented) The security module according to claim 33, wherein said irreversibly writing of said indicator is performed by executing a microprogrammed instruction.

38. (Previously Presented) The security module according to claim 29, wherein said security module is a microcircuit card.

39. (Currently Amended) The method according to claim 23, wherein bothsaid first and second logic operators are parity generators each having two logic opposite outputs and one logic selection input that determines the onewhich of said bothtwo logic opposite outputs [[which]] is input[[ted]] in the comparator.

40. (New) The method according to claim 39, wherein said logic selection input of the comparators is set to a calculation data whose value varies as a function of time.

41. (New) The method according to claim 39, wherein said logic selection input of the comparators is set to a calculation data whose value varies randomly.

42. (New) The method according to claim 20, wherein when determining of a specific condition for the integrity of said information, at least two software instructions of the storage means are executed by processing means for determining said specific condition.

43. (New) The method according to claim 20, wherein when determining of a specific condition for the integrity of said information, the means for checking integrity of information comprise a specific hardware circuit for checking integrity of information in entry of the data bus and at output of the data bus.

44. (New) The security module according to claim 29, wherein the means for checking the integrity comprise at least two software instructions executed by the processing means for verifying said specific condition for integrity.

45. (New) The security module according to claim 29, wherein the means for checking the integrity comprise a specific hardware circuit for checking integrity of information in entry of the data bus and at output of the data bus for verifying said specific condition for integrity.